16

Il Regolamento sulla protezione dei dati personali UE 2016/679 e adempimenti per gli Studi Professionali

aggiornata con il d.lgs. n. 101/2018

Guida informativa.

E.BI.PRO.
ENTE BILATERALE NAZIONALE
PER GLI STUDI PROFESSIONALI

IL REGOLAMENTO SULLA PROTEZIONE DEI DATI PERSONALI UE 2016/679: ADEMPIMENTI PER GLI STUDI PROFESSIONALI

Giuseppe Cassano e Stefano Previti*

Sommario: 1. I principi generali del Regolamento UE 2016/679 e le novità introdotte dal d.lgs. n. 101/2018 - 2. I ruoli nella protezione dei dati personali - 3. *Accountability* - 4. *Privacy by design e privacy by default* - 5. Il *Data Protection Officer (DPO)* - 6. Registro dei trattamenti - 7. Valutazione di impatto (DPIA) - 8. *Data breach* - 9. Consenso - 10. Informativa - 11. Diritti dell'interessato

1. I principi generali del Regolamento UE 2016/679 e le novità introdotte dal d.lgs. n. 101/2018

Il **Regolamento europeo** per la protezione dei **dati personali 2016/679** ("Regolamento" o "GDPR"), come noto **obbligatorio in tutti i Paesi membri dell'Unione Europea a partire dal 25 maggio *u.s.***, raccoglie l'esperienza maturata in Europa negli ultimi venti anni, proponendosi di armonizzare la disciplina della *privacy* a livello comunitario, nell'ottica di individuare un'unica norma uniforme quale minimo comune denominatore fra i 28 Stati membri.

Proprio nel solco di tale principio, l'Italia, con il **decreto legislativo di armonizzazione del 10 agosto 2018, n. 101**, pubblicato in *Gazzetta Ufficiale* il 4 settembre *u.s.*, ha emendato il d.lgs. n. 196/03 ("Codice Privacy"). Con il decreto di recentissima pubblicazione, il quadro normativo in materia di protezione dei dati personali è completo, fugando alcuni dubbi emersi nell'applicazione del Regolamento.

Diversamente da quanto accaduto in epoca precedente, il legislatore comunitario ha inteso considerare il diritto alla protezione dei dati personali **oggetto di bilanciamento di interessi**, anche e soprattutto alla luce della sua **funzione sociale**.

Il **trattamento dei dati personali**, pertanto, dovrà essere, in ogni occasione, **contemperato con i diritti fondamentali**, in ottemperanza al principio di proporzionalità, ma anche con le norme poste a tutela di diritti prevalenti (tra cui, l'interesse pubblico alla trasparenza e all'efficacia della Pubblica Amministrazione) e con le norme civilistiche in tema di negozi giuridici.

* **Giuseppe Cassano**, Avvocato, già Docente di Istituzione di Diritto privato nell'Università LUISS di Roma; Direttore del Dipartimento di Scienze Giuridiche di Roma e Milano della European School of Economics.
Stefano Previti, Avvocato, membro di UIA (Union Internacional des Avocats).

Siamo davanti ad un **cambiamento epocale** in materia di protezione dei dati personali, in quanto il Regolamento mira a raggiungere concretamente la **tutela** del **diritto** dell'interessato al **controllo** sui propri **dati personali**: il tutto **affidando a ogni singolo titolare le scelte** per garantire detto diritto.

Le principali **novità** introdotte dal Regolamento sono rappresentate da:

1. principio di ***accountability*** o "responsabilizzazione/rendicontazione";
2. introduzione dei principi di ***privacy by design*** e ***privacy by default***;
3. previsione della figura del ***Data Protection Officer*** (non del tutto sconosciuta nel nostro ordinamento, ma sicuramente la figura protagonista del GDPR);
4. **registro dei trattamenti**;
5. **valutazione di impatto (DPA)**;
6. procedura di ***data breach***;

ma anche…

7. rilascio del **consenso** e la possibilità per i minori di prestare validamente il proprio consenso per i servizi della società dell'informazione (quali ad esempio Facebook, Instagram, ecc.);
8. contenuto dell'**informativa**;
9. nuovi **diritti dell'interessato** (*portability*, diritto all'oblio, diritto all'accesso, ecc.).

Come appena menzionato, il **decreto legislativo n. 101/2018** è intervenuto al fine di **coordinare** il **Codice Privacy** a tali **novità**, mettendo a punto quelle precisazioni che lo stesso Regolamento demandava alla scelta discrezionale dei singoli Paesi membri.

Tra le ulteriori novità, dunque, si segnalano:

a) la previsione per cui, per i **primi otto mesi** dall'entrata in vigore del Regolamento (dunque sino al **maggio 2019**), nell'**erogare le sanzioni**, il Garante per la protezione dei dati personali tiene conto del fatto di essere ancora in una fase iniziale di attuazione della normativa;

b) il **consenso** dei **minori italiani** sin dall'età dei **14 anni** per il trattamento dei dati personali nella fruizione dei servizi della società dell'informazione (sul punto, il GDPR ha lasciato margine ai singoli Stati membri per stabilire l'età per il rilascio del consenso da parte del minore, in un *range* dai 13 sino ai 16 anni; in Francia, ad esempio, il progetto di legge individua come età idonea per il rilascio del consenso i 15 anni);

c) la possibilità, per il titolare e il responsabile, di **nominare persone fisiche** espressamente **designate** per **svolgere specifici compiti e funzioni** in relazione al trattamento dei dati personali;

d) la previsione per cui, nei casi di ricezione dei ***curricula*** spontaneamente trasmessi dai candidati, al fine della instaurazione di un rapporto di lavoro, l'informativa deve esser fornita al momento del primo contatto utile, successivo all'invio del *curriculum*. Peraltro, il consenso al trattamento dei dati personali presenti nei *curricula* non è dovuto;

e) la **limitazione dei diritti** degli interessati, ad integrazione dei casi già presenti nel Regolamento (art. 23), in determinate ipotesi di cui si dirà *infra*;

f) la gestione dei **diritti** riguardanti le **persone decedute**, che possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.

I **destinatari** delle novità apportate dal Regolamento e dal decreto di armonizzazione – che verranno illustrate nel prosieguo – sono:

- le **aziende**;
- le **Pubbliche Amministrazioni**;
- gli **studi professionali**.

Il concetto di **protezione del dato** (inteso non solo nella sua rappresentazione in forma digitale), in tutto il suo **ciclo vitale**, deve rappresentare una **priorità** nelle **strategie di gestione del rischio** anche degli **studi professionali**, stante la delicatezza dei dati trattati. Si pensi, ad esempio, ai dati relativi alla salute trattati dagli **studi medici**, ai dati giudiziari trattati dagli **avvocati**, ai dati relativi all'appartenenza sindacale degli interessati trattati dai **consulenti del lavoro** e così via.

Il Regolamento, dunque, prevede che anche gli studi professionali, in qualità di titolari o responsabili, devono adottare misure organizzative e tecniche idonee a garantire un **livello di sicurezza adeguato al rischio sia informatico che legale**, legato al trattamento del dato: dunque non si può prescindere da una puntuale **analisi del rischio** di ogni trattamento.

Pertanto, anche gli **studi professionali devono adeguarsi al Regolamento**, che non dovrà esser visto solo come un obbligo, ma come un'opportunità per migliorare l'efficienza della propria organizzazione.

Ciò premesso, si illustreranno di seguito le principali novità apportate dal GDPR e recepite dal Codice Privacy per come emendato dal decreto di armonizzazione, indicando cosa sarebbe opportuno porre in essere.

2. I ruoli nella protezione dei dati personali

Prima di addentrarci nell'analisi delle principali novità della normativa, appare opportuno soffermarsi, seppur in forma sintetica, sui **ruoli del trattamento dei dati personali**, anche al fine di meglio comprendere in che termini e per quali finalità è intervenuto il legislatore comunitario con questo Regolamento.

I ruoli maggiormente rilevanti sono:

i. il **Titolare**;
ii. il **Responsabile**;
iii. il "**sub-Responsabile**";
iv. il ***Data Protection Officer*** **(DPO)**.

Il decreto attuativo del Regolamento ha abrogato il Titolo IV del Codice Privacy, rubricato "*Soggetti che effettuano il trattamento*", e dunque dovendosi,

ad oggi, far riferimento alla sola fonte comunitaria per ottenere l'esatta definizione dei ruoli della *privacy*.

Il **Titolare** del trattamento è la persona fisica o giuridica che determina le **finalità** e i **mezzi del trattamento** di dati personali (sono qualificabili, ad esempio, come titolare la società, l'associazione professionale, l'avvocato, il commercialista, la fondazione, il consiglio dell'ordine, ecc.).

Egli è tenuto ad adottare, e a dimostrare di aver adottato (e tanto in ottemperanza al principio di *accountability*, di cui si dirà a breve), tutte le **misure necessarie** a **garantire** la **conformità del trattamento al GDPR**, tenuto conto del contesto complessivo in cui si svolge il trattamento, nonché dei rischi per i diritti e le libertà degli interessati.

Il Regolamento, all'art. 26, prevede che in ogni caso in cui le finalità ed i mezzi del trattamento vengano determinati **congiuntamente** da parte di più titolari, potrà essere nominato uno o più "**contitolare/i**" del trattamento: il rapporto interno tra contitolari deve essere disciplinato da apposito accordo (reso disponibile a tutti gli interessati) avente ad oggetto le rispettive responsabilità e le rispettive funzioni di comunicazione delle informazioni.

Il **Responsabile** del trattamento è la persona fisica o giuridica che **tratta dati personali per conto del Titolare del trattamento**. La **nomina** del Responsabile del trattamento deve avvenire con apposito atto scritto, contratto, o comunque per clausole tipizzate, e deve contenere gli elementi individuati dall'art. 28 del GDPR e tassativamente almeno le materie riportate al paragrafo 3 della medesima disposizione, al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" – quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, e categorie di dati oggetto di trattamento; le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel Regolamento –[1]. Si ribadisce che la figura di responsabile prevista dal Regolamento dovrebbe intendersi come **figura esterna all'organizzazione del Titolare**, sì da poterlo definire come "responsabile esterno", rispetto all'organizzazione del titolare; tipicamente saranno nominati responsabili ai sensi dell'art. 28 del Regolamento le società informatiche, i commercialisti, ecc. Il Responsabile può, a sua volta, nominare un **sub-Responsabile**, ma solo previa specifica autorizzazione (generale o specifica) da parte del Titolare del trattamento.

Si badi come il GDPR, con riferimento alla figura del Responsabile, abbia espresso preferenza per una "**esternalizzazione**": la previsione di apposita nomina (mediante atto/contratto) e la tipizzazione degli elementi che tale nomina dovrà contenere è indirizzata a consentire di individuare la figura del Responsabile in un soggetto esterno alla società.

1 Sul punto si veda anche l'*Opinion* 1/2010 del *Working Part* 29, la quale chiarisce molto bene i casi in cui sussiste la contitolarità, oppure il rapporto titolare/responsabile.

Dunque, lo **studio professionale** – in qualità di Titolare – nel momento in cui affiderà la gestione di alcuni dati personali a soggetti terzi (come la società che gestisce i servizi informatici) dovrà nominarli, mediante atto di nomina o contratto, come Responsabile ai sensi dell'art. 28 del GDPR.

Chiarito detto aspetto, il Regolamento prevede la possibilità per il Titolare e per il Responsabile di avvalersi di **persone autorizzate** "*al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*". Ci si riferisce a categorie di **soggetti interni**, che ben potrebbero figurare nell'organigramma come **dipendenti** e **collaboratori**, i quali sono tenuti ad eseguire le operazioni di trattamento secondo le finalità e le istruzioni impartite, ad assicurarsi che l'esecuzione delle operazioni di trattamento avvenga nel pieno rispetto dei principi generali del GDPR e ad adottare tutte le cautele necessarie ad evitare rischi di violazioni di dati (pertanto, anche nel caso di *data breach*). Tale previsione è stata confermata anche dal Codice Privacy (v. *supra*, paragrafo 1, lett. c).

Il Titolare e il Responsabile, oltre ad impartire specifiche istruzioni, dovranno preoccuparsi anche di **formare ciclicamente** le persone autorizzate sul GDPR, in modo che le stesse possano consapevolmente applicare la normativa in esame negli studi professionali.

Il ***Data Protection Officer*** **(DPO)** è una nuova figura, introdotta dal GDPR, di tipo manageriale, che supporta l'attività del Titolare nel rispetto delle prescrizioni in tema di protezione dei dati, nonché nella supervisione dei profili di responsabilità giuridica derivanti dall'applicazione del principio di *accountability* (su tale figura si dirà *amplius infra*).

In ogni caso, sarà il Titolare a dover costruire – previa analisi delle proprie esigenze e specifica valutazione – il proprio organigramma *privacy* ed il proprio sistema di gestione della stessa.

3. *Accountability*

Il **principio di *accountability***, anche principio di rendicontazione o di responsabilità, impone al titolare del trattamento dati di dimostrare di aver adottato un processo complessivo di **misure giuridiche, amministrative, tecniche, per la protezione dei dati personali raccolti, anche attraverso l'elaborazione di specifici modelli organizzativi**.

Sono i titolari, nella nuova disciplina, a decidere autonomamente le modalità, le garanzie ed i limiti stessi del trattamento dei dati personali, a differenza di quanto accadeva prima dell'entrata in vigore del Regolamento, quando, difatti, la liceità di particolari tipologie di trattamento veniva subordinata all'autorizzazione dell'Autorità Garante per la protezione dei dati personali ("Garante Privacy"). L'intervento dell'Autorità è adesso principalmente *ex post*, ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare. In particolare detto principio richiede la **proattività** del titolare il quale non dovrà più attenersi a misure minime previste dal Legislatore, ma dovrà porre in essere

scelte per garantire la conformità al GDPR. Già da questo principio si coglie la portata rivoluzionaria del GDPR: è il titolare che – attraverso un *self regulation* – deve individuare e porre in essere le migliori scelte per raggiungere l'obiettivo indicato dalla normativa.

Cosa devono fare gli studi professionali?

4. *Privacy by design e privacy by default*

Espressione del principio di *accountability,* sono i principi di *privacy by design* e *privacy by default*.

In base al primo, il titolare del trattamento è tenuto ad adottare misure di **pseudonimizzazione** – ovvero misure tali da consentire la conservazione dei dati in forma anonima – e **minimizzazione del trattamento dei dati**, nonché di **protezione dei dati sin dalla progettazione del trattamento**, tenuto conto del contesto complessivo in cui si svolge il trattamento, nonché dei rischi (previa **valutazione del rischio**) per i diritti e le libertà degli interessati.

Il principio di ***privacy by default*** stabilisce, invece, che per impostazione predefinita il titolare deve trattare **solo** ed **esclusivamente** i **dati personali** nella **misura necessaria** e **sufficiente** per le **finalità previste** e per il **periodo strettamente necessario** a tali fini. Occorre, quindi, progettare il sistema di trattamento di dati garantendo la **non eccessività dei dati raccolti.**

Tale previsione si sostanzia nell'adempimento, da parte del titolare, di una serie di attività specifiche e dimostrabili, da effettuarsi *ex ante*, ossia prima di procedere al trattamento vero e proprio.

Cosa devono fare gli studi professionali?

5. Il *Data Protection Officer* (DPO)

Il Regolamento introduce, agli artt. 37-39, la figura del ***Data Protection Officer*** (il "**DPO**") che può esser considerato un ***manager*** **della protezione dei dati**.

Il DPO è una **figura autonoma ed indipendente di controllo**, di **consulenza** e di **supporto** al titolare ed al responsabile del trattamento, per l'**applicazione concreta all'interno degli studi professionali del GDPR**. Peraltro, il DPO sarà il punto di contatto tra lo studio professionale ed il Garante e gli interessati.

Ogni studio professionale dovrà valutare puntualmente se è obbligato o meno a nominare un DPO, tenendo conto di quanto disposto dal Regolamento all'art. 37, ove sono previsti **i casi** in cui la **nomina è obbligatoria**. Sono rilevanti per gli studi professionali le seguenti previsioni:

"*b) se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il* ***monitoraggio regolare*** *e* ***sistematico di interessati*** *su larga scala;*

c) se le attività principali del titolare o del responsabile consistono nel trattamento su ***larga scala*** *di categorie particolari di dati, come quelli* ***biometrici, sanitari, genetici o di dati personali relativi a condanne penali e reati.***" [2].

[2] **Per monitoraggio 'regolare'** si intende:
- in corso o che si verifica a intervalli specifici per un determinato periodo;
- ricorrente o ripetuto in tempi fissi;
- costante o periodico.

Per monitoraggio 'sistematico' si intende un trattamento che:
- si svolge attraverso un sistema, una strategia, preorganizzato, organizzato o metodico;
- si svolge nell'ambito di un piano generale per la raccolta dei dati (es. salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; ecc.).

Per trattamenti su 'larga scala' devono essere tenuti in considerazione:
- il numero degli interessati coinvolti;
- il volume dei dati trattati;
- la durata delle attività di trattamento o l'estensione geografica del trattamento.

In particolare, con riferimento al **trattamento "su larga scala"**, i Garanti Europei hanno precisato che esso deve considerarsi tale nei seguenti casi:

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di *fast food*;
- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Mentre, esempi di trattamento non su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

Ad esempio, sarà obbligatorio per uno studio professionale che tratta in larga scala dati sanitari provvedere alla nomina di un DPO. Da ultimo, si segnala come il Garante abbia chiarito che **non** ricorre trattamento dati "**su larga scala**", ai fini della nomina del DPO, nel caso in cui l'attività venga posta in essere da liberi professionisti operanti in **forma individuale** (es. il singolo avvocato). Occorrerà, pertanto, nella valutazione sulla necessità della nomina, tenere in debita considerazione la struttura dello studio professionale e la forma in cui la prestazione del servizio è resa (es. società tra avvocati). Si consideri che, anche nell'ipotesi in cui la società tra professionisti abbia una struttura agile, la valutazione sull'obbligatorietà o meno del DPO dovrà esser fatta, in quanto, per l'esenzione, si fa riferimento specificatamente alla "forma individuale".

Ma chi può assumere la funzione di DPO?

Fra le competenze e conoscenze specialistiche richieste per la nomina del DPO rientrano:

a) **conoscenza** della **normativa** e delle **prassi nazionali ed europee** in materia di protezione dei dati;
b) familiarità con le **operazioni di trattamento** svolte;
c) familiarità con **tecnologie informatiche** e **misure di sicurezza dei dati**;
d) conoscenza dello **specifico settore di attività** e dell'organizzazione del titolare/del responsabile;
e) capacità di promuovere una **cultura della protezione dati** all'interno dell'organizzazione del titolare/del responsabile;

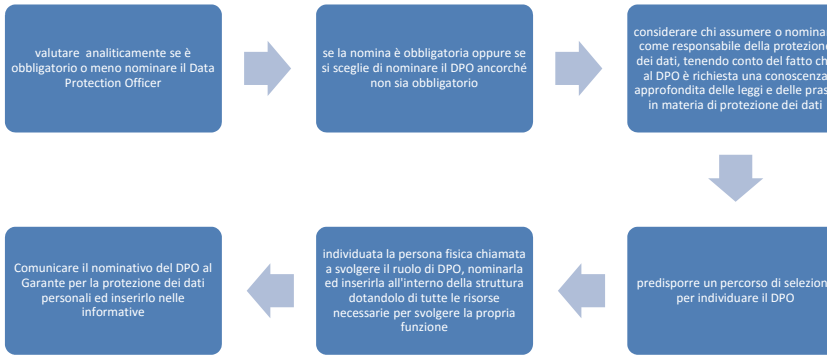
f) capacità di assolvere ai propri compiti e, pertanto, **elevati *standard* deontologici e di professionalità**.

Il Regolamento prevede anche che la funzione di DPO – oltre a poter esser assunta da un dipendente dell'azienda – possa essere svolta in base ad un contratto di servizi stipulato con una persona fisica o giuridica esterna all'organismo o all'azienda titolare/responsabile del trattamento.

Il DPO, dunque, oltre ad esser la figura maggiormente nota introdotta dal GDPR, è anche la più dibattuta e richiesta dal mercato. Infatti, oltre ad esserci numerose offerte per detta figura, una delle domande più comuni riguarda i **requisiti professionali** e le **certificazioni** che il **DPO deve avere**.

Il Regolamento, le Linee Guida dei Garanti Europei (WP 243) e il Garante per la *privacy* italiano hanno chiarito che le certificazioni diffuse sul mercato (che non rientrano tra quelle disciplinate dal Regolamento), pur rappresentando, al pari di altri titoli, uno strumento valido ai fini della verifica del possesso di un livello minimo di conoscenza della disciplina, tuttavia non equivalgono, di per sé, a una "abilitazione" allo svolgimento del ruolo del DPO. Dunque, **non sono indispensabili certificazioni per ricoprire il ruolo del DPO**, mentre è assolutamente necessaria una conoscenza e competenza specialistica della normativa in materia di protezione dei dati, nonché una conoscenza dell'ambito di operatività e del *core business* dello studio professionale dove il DPO svolgerà la propria attività.

Cosa devono fare gli studi professionali per nominare il DPO?



6. Registro dei trattamenti

Il Regolamento prevede che tutti i titolari ed i responsabili del trattamento che abbiano oltre 250 dipendenti predispongano un **registro delle operazioni del**

trattamento, i cui contenuti sono indicati all'art. 30: trattasi non di un mero adempimento formale, bensì di parte integrante di un sistema di corretta gestione dei dati personali, in quanto volto proprio a tener sotto controllo il **ciclo vitale del dato**.

Dunque, **anche nell'ipotesi in cui non sia obbligatorio adottare il registro dei trattamenti sarebbe opportuno implementarlo**, in quanto strumento utile per censire tutti i trattamenti operati dagli studi professionali.

Quali informazioni deve avere il registro dei trattamenti predisposto dal titolare?

La compilazione del registro può essere fatta con vari strumenti: dal foglio *excel* a *software* sviluppati *ad hoc*.

Il registro deve contenere una descrizione dei principali elementi dei trattamenti svolti, e segnatamente:

a) il nome e i dati di contatto del titolare/contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di Paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale, compresa l'identificazione del Paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Quali informazioni deve avere il registro dei trattamenti predisposto dal responsabile?

Il **responsabile del trattamento** è tenuto a tenere un apposito registro di tutte le categorie di attività relative al trattamento, svolte per conto di un titolare del trattamento, contenente:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile, del rappresentante del titolare del trattamento o del responsabile del trattamento e del responsabile dei dati;

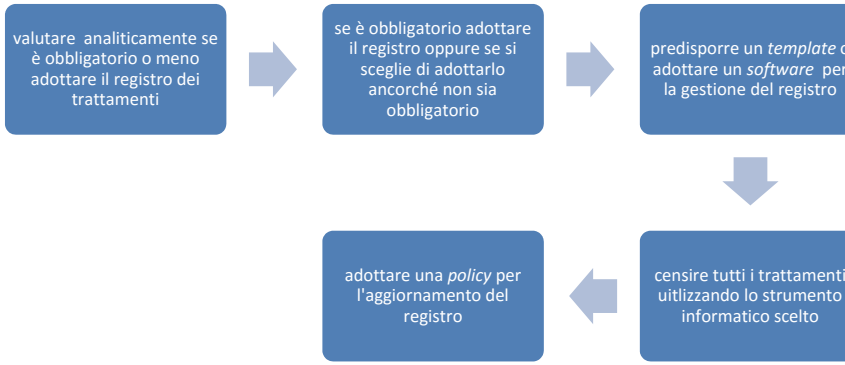
b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale, compresa l'identificazione del Paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'art. 49 (trasferimento da un registro che mira a fornire informazioni al pubblico e può essere consultato da chiunque sia in grado di dimostrare un legittimo interesse), la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure tecniche e organizzative.

Quindi ogni organizzazione potrà avere due registri uno in qualità di titolare e uno in qualità di responsabile.

Cosa fare in merito al registro del trattamento?



7. Valutazione di impatto (DPIA)

L'articolo 35 del Regolamento introduce, invece, l'istituto della **valutazione d'impatto** per i trattamenti che presentano **rischi specifici**, anche conosciuta come ***Data Privacy Impact Assessment*** ("**DPIA**"): è un processo inteso a descrivere il trattamento, a valutarne la necessità e la proporzionalità alla gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.

La DPIA è uno strumento importante per la **responsabilizzazione**, in quanto sostiene i titolari del trattamento non soltanto nel rispettare i requisiti, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto

del Regolamento[3]. In altre parole, la **valutazione d'impatto** sulla protezione dei dati è un **processo inteso a garantire e dimostrare la conformità al GDPR** e proprio per tale ragione i Garanti Europei con le Linee Guida in materia (WP248) suggeriscono di valutarne l'impiego per tutti i trattamenti, e non solo nei casi in cui il Regolamento ne prescriva l'obbligatorietà.

La **valutazione d'impatto** è **obbligatoria** ogniqualvolta il trattamento – considerati la natura, l'oggetto, il contesto e le finalità dello stesso preveda l'uso di nuove tecnologie, – "*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*".

La **mancata esecuzione** di una valutazione d'impatto sulla protezione dei dati – nei casi in cui il trattamento è soggetto alla stessa – l'**esecuzione in maniera errata** di detta valutazione oppure la **mancata consultazione dell'Autorità di controllo** – laddove richiesto – possono comportare una **sanzione amministrativa pecuniaria pari a un importo massimo di 10 milioni di euro oppure, nel caso di un'impresa, pari a fino al 2% del fatturato annuo globale dell'anno precedente**, a seconda di quale dei due importi sia superiore.

Il titolare del trattamento, laddove ritenesse che il rischio non possa essere ragionevolmente attenuato in termini di tecnologie disponibili e di costi di attuazione, e dovesse risultare dalla valutazione d'impatto che il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, dovrà ricorrere alla **consultazione preventiva dell'Autorità di Controllo** – di cui all'art. 36 del Regolamento – tenendo presente che la pseudonimizzazione e la cifratura dei dati personali non costituiscono necessariamente misure idonee.

Inoltre, vi sono **ipotesi di esonero della valutazione d'impatto**: in particolare, i Garanti Europei, nell'interpretare la norma, hanno precisato come una DPIA non sia obbligatoria per tutte quelle operazioni in cui il trattamento non presenti rischi elevati per l'interessato, e nello specifico nei seguenti casi (a mero titolo esemplificativo e non esaustivo):

- se il trattamento non "*può comportare un rischio elevato per i diritti e le libertà di persone fisiche*" [4];
- se la natura, l'ambito, il contesto e le finalità del trattamento sono molto simili a quelli del trattamento per cui è già stata condotta una DPIA[5];
- se il trattamento è stato sottoposto a verifica da parte di un'autorità di controllo prima del 25 maggio 2018 in condizioni specifiche che non hanno subito modifiche[6].

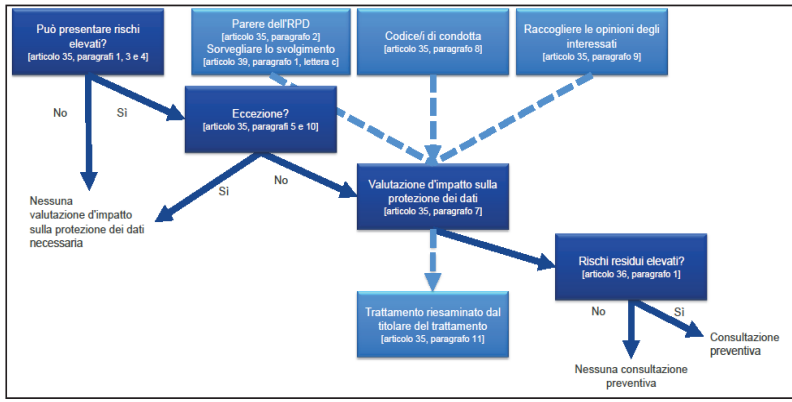
[3] Ciò anche in considerazione del considerando 84, a mente del quale: "*[l]'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento*", nonché dell'art. 24 del GDPR.

[4] Cfr. Art. 35, paragrafo 1 del Regolamento.

[5] Cfr. Art. 35, paragrafo 1 del Regolamento.

[6] Cfr. Considerando 171.

Di seguito si riepilogano i principi fondamentali relativi alla valutazione d'impatto sulla protezione dei dati:



La valutazione di impatto si rende obbligatoria nei casi di:

- valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la **profilazione**, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- trattamento, su larga scala, di **categorie particolari di dati personali**;
- sorveglianza sistematica su larga scala di una **zona accessibile al pubblico**.

Anche gli **studi professionali** dovranno valutare, sulla base dei trattamenti effettuati (e, dunque, dei dati trattati), se la valutazione d'impatto è richiesta. Ad esempio, una valutazione di impatto potrebbe rendersi necessaria laddove lo studio tratti **particolari categorie di dati** (che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) "su larga scala" (si veda *sub* par. 3 in nota), oppure tratti dati relativi a **interessati vulnerabili** come i **minori** e i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.); oppure il trattamento abbia ad oggetto una notevole quantità di dati personali e un vasto numero di interessati. Ulteriori esempi possono esser individuati in uno studio medico associato che conserva le cartelle cliniche dei pazienti oppure in quello di un investigatore privato che conserva i dettagli dei trasgressori.

Come si svolge una valutazione d'impatto?

La **DPIA** deve essere **condotta** "*prima di procedere al trattamento*", e quindi sin **dalla fase di progettazione**.

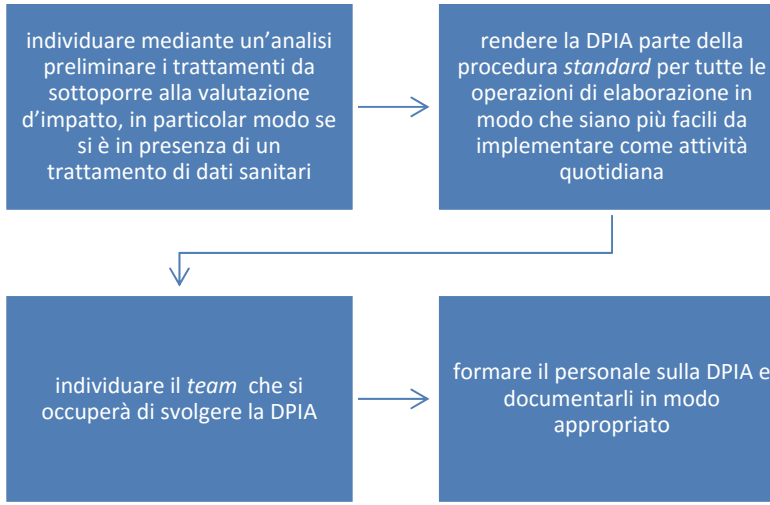
La DPIA rappresenta un processo continuativo che necessita, talvolta, un aggiornamento anche dopo l'inizio effettivo del trattamento, dovendo la **DPIA effettuarsi** a **intervalli regolari**.

Tale **processo** viene **condotto dal titolare** – anche se la conduzione materiale della valutazione d'impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione – **insieme al DPO** ed **al responsabile**.

In particolare, il titolare ne monitora lo svolgimento, consultandosi con il responsabile della protezione dei dati e acquisendo – se i trattamenti lo richiedono – il parere di esperti di settore, del responsabile della sicurezza dei sistemi e del responsabile IT.

Possiamo sintetizzare il processo iterativo generale, relativo alla conduzione di una DPIA in sette punti, così come di seguito illustrato graficamente:

Cosa fare?



Si segnala che l'Autorità per la protezione dei dati personali francese (CNIL) ha messo a disposizione gratuitamente sul proprio portale un software anche in lingua italiana per poter svolgere la valutazione d'impatto (disponibile all'indirizzo *https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment*).

8. *Data breach*

L'articolo 33 del Regolamento **obbliga** tutti i titolari del trattamento (indipendentemente da dimensione e settore di intervento) a **notificare** la **violazione** dei dati personali all'**Autorità Garante entro 72 ore** dal momento in cui si è venuti a conoscenza del fatto, ovvero nel momento in cui il titolare ne è reso consapevole[7], **senza ingiustificato ritardo**, **tenendo conto**, in particolare, **della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato**.

Se la **violazione** è suscettibile di **comportare** un **rischio elevato** per i **diritti** e le **libertà** delle **persone fisiche**, il **titolare** deve **comunicare** la **violazione all'interessato senza ingiustificato ritardo**[8].

[7] "*Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo*", cfr. art. 33 del GDPR.

[8] La comunicazione dovrebbe essere data direttamente e personalmente all'interessato coinvolto dalla violazione, a meno che ciò comporti sforzi sproporzionati. In tal caso, si procede invece ad una comunicazione pubblica o a una misura

L'obbligo di comunicazione[9] risponde allo **scopo** di consentire all'interessato – qualora sussista una siffatta violazione – di **prendere** le **precauzioni necessarie** per **dirimere** quanto più possibile gli **effetti**.

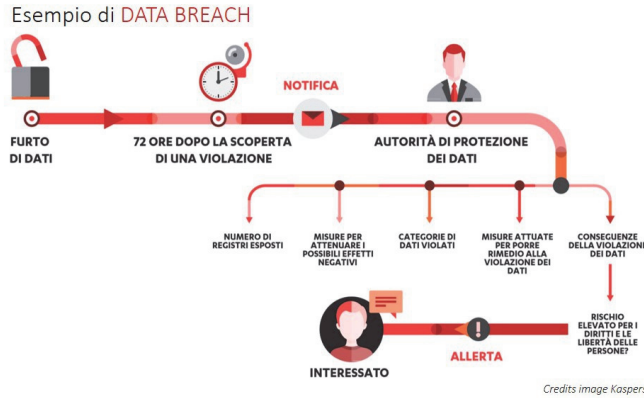
La comunicazione del *data breach* all'interessato deve essere effettuata con un **linguaggio semplice e chiaro**[10] e deve contenere la **descrizione** e la **natura** della violazione dei dati personali con le possibili **conseguenze.**

Il titolare del trattamento è pertanto **esentato** dall'effettuare la notifica solo se è in grado di dimostrare che la violazione dei dati personali non presenta rischi per i diritti dell'interessato e di aver adempiuto ai suoi compiti mettendo in atto:

- misure di sicurezza tecniche e organizzative preventive idonee a proteggere i dati personali in caso di *data breach*;
- misure di sicurezza tecniche e organizzative successive al *data breach*, idonee a prevenire un rischio elevato per i diritti e le libertà degli interessati.

Il rischio di non ottemperare a detta prescrizione è molto alto in quanto le **sanzioni** – anche per gli studi professionali – possono arrivare sino a **10 milioni di euro o il 2% del fatturato mondiale**, se superiore.

Di seguito si illustra graficamente la procedura per il *data breach*:



Credits image Kaspersky

simile, tramite la quale gli interessati sono informati con la medesima efficacia.

9 Articolo 34 del Regolamento.

10 In merito a tale aspetto, le Linee Guida WP 250 (cfr. pag. 21) precisano che comunicazioni di tal sorta non devono essere inviate agli interessati unitamente ad altre informazioni, come aggiornamenti *regolari*, *newsletter* o messaggi *standard*. Si aggiunge, inoltre, che metodi di comunicazione trasparenti – e quindi preferibili – potrebbero essere individuati, ad esempio, in *e-mail*, SMS, notifiche in primo piano.

Cosa devono fare gli studi professionali?

9. Consenso

Il consenso dell'interessato è *"**qualsiasi manifestazione di volontà***" con la quale l'interessato medesimo presti, in maniera **libera, specifica, informata ed inequivocabile**, il proprio "*assenso (...) che i dati personali che lo riguardano siano oggetto di trattamento*", ricorrendo ad una dichiarazione o, in alternativa, ad una "*azione positiva inequivocabile*".

Il Considerando 32 del Regolamento chiarisce che il consenso può intendersi prestato in "***un atto positivo ed inequivocabile***", in forma di:

- *dichiarazione scritta* (ma non necessariamente sottoscritta) approntata anche con mezzi elettronici;
- *dichiarazione orale*;
- o, ancora, *azione positiva non dichiarativa, ma pur sempre inequivocabile*, in ordine all'accettazione dell'interessato.

Dunque, silenzio, caselle pre-spuntate e inattività non saranno sufficienti a dimostrare il consenso dell'interessato al trattamento del dato.

Per i dati di cui all'art. 9 del Regolamento (Categorie particolari di dati) – quali, ad esempio, i dati sanitari, i dati biometrici e genetici, i dati giudiziari – il Regolamento prevede che il consenso debba essere "**esplicito**", e tanto vale anche con riguardo alle decisioni basate su trattamenti automatizzati.

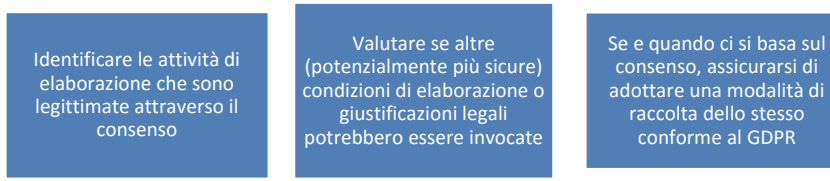
Per contro, il consenso **non deve essere necessariamente documentato per iscritto**, né viene prevista la forma scritta *ad substantiam* per particolari categorie di dati. Ciò che viene posto in rilievo dal Regolamento è la **necessità di documentare** l'attività di trattamento svolta: in tale ottica, il titolare deve essere in grado di **dimostrare** che l'interessato ha prestato il consenso a uno specifico trattamento.

Ulteriore **novità** introdotta dal Regolamento in materia di consenso è la previsione della **validità del consenso dei minori** che, nella formulazione

comunitaria, sono legittimati a prestarlo a partire dai 16 anni: in tal modo, diversamente da quanto previsto dalla normativa previgente, con riferimento alle attività connesse alla società dell'informazione (uso dei *social network* e di applicazioni quali Facebook, Instagram, ecc.), i minori potranno decidere autonomamente sul trattamento dei propri dati.

Il legislatore italiano ha scelto di esercitare il proprio margine di discrezionalità riconosciuto dal Regolamento ai singoli Stati membri per abbassare ulteriormente l'età del consenso: in **Italia**, dunque, il **consenso del minore**, per i servizi della società dell'informazione, è **valido sin dai 14 anni**.

Cosa fare?



10. Informativa

Agli articoli 13, comma 1, e 14, comma 1, il Regolamento indica in modo tassativo i **contenuti dell'informativa** da presentare all'interessato.

In particolare, il titolare deve sempre specificare:

- i dati di contatto del DPO, ove presente;
- la base giuridica del trattamento;
- l'interesse legittimo sotteso al trattamento, ove presente;
- l'eventuale trasferimento di dati a Paesi terzi e, in tal caso, gli strumenti impiegati per il trasferimento;
- il periodo di conservazione dei dati o il criterio impiegato per la definizione del periodo di conservazione;
- il diritto di presentare reclamo all'autorità di controllo;
- in caso di impiego di processi decisionali automatizzati, la logica di tali processi e le conseguenze previste per l'interessato.

L'informativa dovrà, dunque, essere resa in **forma concisa, trasparente, comprensibile per l'interessato e facilmente accessibile**. Dovrà, inoltre, essere fornita **entro un termine ragionevole** che non potrà superare un mese dalla raccolta, oppure **al momento della comunicazione dei dati**.

Alla luce di tali espresse prescrizioni, **gli studi professionali che non l'abbiano già fatto dovranno verificare la rispondenza delle informative**

attualmente impiegate ai nuovi criteri, in modo tale da poter apportare eventuali modifiche e/o integrazioni necessarie.

Si segnala che il decreto di armonizzazione ha introdotto l'art. 111-*bis,* secondo cui, nei casi di **ricezione dei *curricula*** spontaneamente trasmessi dai candidati, al fine della **instaurazione di un rapporto di lavoro**, l'informativa deve esser fornita al momento del primo contatto utile, successivo all'invio del *curriculum*. Peraltro, il consenso al trattamento dei dati personali presenti nei *curricula* non è dovuto.

Di seguito si indica una *check list*, non esaustiva nel suo contenuto, per predisporre un'informativa ai sensi dell'art. 13 del GDPR.

Domande	Risposte *[si/no/commenti]*
Hai indicato l'identità e i dati di contatto del titolare e del DPO?	
Hai indicato le finalità del trattamento?	
Hai indicato i diritti di cui gode l'interessato *ex* artt. 15-22 GDPR?	
Hai indicato il periodo di conservazione dei dati?	
Hai indicato le modalità del trasferimento dei dati presso Paesi Terzi?	
Hai indicato la sussistenza di profilazione?	
Il contenuto dell'informativa è chiaro, conciso e facilmente accessibile?	
Le informazioni rese all'interessato sono concrete?	
Le informazioni rese all'interessato sono astratte e/o ambivalenti?	
L'informativa è costantemente disponibile e reperibile?	
L'informativa è stata predisposta nel modo più semplice possibile, senza ricorrere a periodi complessi e/o linguaggi strutturati?	

FAC-SIMILE DI INFORMATIVA

Oggetto: Informativa ai sensi dell'articolo 13 del Regolamento UE n. 2016/679
Ai sensi dell'art. 13 del Regolamento UE n. 2016/679 (di seguito "GDPR"o "Regolamento"), recante disposizioni a tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, desideriamo informarLa che i dati personali da Lei forniti formeranno oggetto di trattamento nel rispetto della normativa sopra richiamata e degli obblighi di riservatezza cui è tenuta lo Studio [•].

Titolare del trattamento
Il Titolare del trattamento è lo Studio [•] di [•], nella persona [•] domiciliato per la carica in [•] alla Via [•]

Responsabile della protezione dei dati (DPO)
Il responsabile della protezione dei dati (DPO) è [•] Via [•] Il Responsabile del trattamento è [•] indirizzo *e-mail* [•]

Finalità del trattamento
I dati personali da Lei forniti sono necessari per [•]

Modalità di trattamento e conservazione
Il trattamento sarà svolto in forma automatizzata e/o manuale, nel rispetto di quanto previsto dall'art. 32 del GDPR in materia di misure di sicurezza, ad opera di soggetti appositamente incaricati e in ottemperanza a quanto previsto dall'art. 29 del Regolamento.
Le segnaliamo che, nel rispetto dei principi di liceità, limitazione delle finalità e minimizzazione dei dati, ai sensi dell'art. 5 GDPR, previo il Suo consenso libero ed esplicito espresso in calce alla presente informativa, i Suoi dati personali saranno conservati per il periodo di tempo necessario per il conseguimento delle finalità per le quali sono raccolti e trattati.

Ambito di comunicazione e diffusione
Informiamo inoltre che i dati raccolti non saranno mai diffusi e non saranno oggetto di comunicazione senza Suo esplicito consenso, salvo le comunicazioni necessarie che possono comportare il trasferimento di dati ad enti pubblici, a consulenti o ad altri soggetti per l'adempimento degli obblighi di legge.

Trasferimento dei dati personali
I suoi dati non saranno trasferiti né in Stati membri dell'Unione Europea né in Paesi terzi non appartenenti all'Unione Europea.

Categorie particolari di dati personali
Ai sensi degli articoli 9 e 10 del Regolamento, Lei potrebbe conferire dati qualificabili come "categorie particolari di dati personali" e cioè quei dati che rivelano "*l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*". Tali categorie di dati potranno essere trattate dallo Studio solo previo Suo libero ed esplicito consenso, manifestato in forma scritta in calce alla presente informativa.

Esistenza di un processo decisionale automatizzato, compresa la profilazione
Lo Studio non adotta alcun processo decisionale automatizzato, compresa la profilazione, di cui all'articolo 22, paragrafi 1 e 4, del Regolamento.

Diritti dell'interessato
In ogni momento, Lei potrà esercitare, ai sensi degli articoli dal 15 al 22 del Regolamento, il diritto di:
a) chiedere la conferma dell'esistenza o meno di propri dati personali;
b) ottenere le indicazioni circa le finalità del trattamento, le categorie dei dati personali, i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati e, quando possibile, il periodo di conservazione;
c) ottenere la rettifica e la cancellazione dei dati;
d) ottenere la limitazione del trattamento;
e) ottenere la portabilità dei dati, ossia riceverli da un titolare del trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e trasmetterli ad un altro titolare del trattamento senza impedimenti;
f) opporsi al trattamento in qualsiasi momento ed anche nel caso di trattamento per finalità di *marketing* diretto;
g) opporsi ad un processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione.
h) chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
i) revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
j) proporre reclamo a un'autorità di controllo.

Può esercitare i Suoi diritti con richiesta scritta inviata a [•], all'indirizzo postale [•] o all'indirizzo *e-mail* [•].
Io sottoscritto/a dichiaro di aver ricevuto l'informativa che precede.
Luogo, lì [•]
Io sottoscritto/a alla luce dell'informativa ricevuta
□esprimo il consenso □NON esprimo il consenso al trattamento dei miei dati personali inclusi quelli considerati come categorie particolari di dati.
□esprimo il consenso □ NON esprimo il consenso alla comunicazione dei miei dati personali ad enti pubblici e società di natura privata per le finalità indicate nell'informativa.
□esprimo il consenso □ NON esprimo il consenso al trattamento delle categorie particolari dei miei dati personali così come indicati nell'informativa che precede.

11. Diritti dell'interessato

Il decreto n. 101/2018 ha abrogato il Titolo II del Codice Privacy sui Diritti dell'interessato. Tali diritti vengono disciplinati, ad oggi, dal Regolamento, agli artt. 15 ss. e di seguito si indicano alcune considerazioni sulle più rilevanti novità.

Il **diritto alla portabilità di dati** (art. 20) è tra le principali novità introdotte dal Regolamento e si rappresenta come il diritto per gli interessati di **ricevere i dati personali** da loro forniti al titolare del trattamento, in un **formato "*strutturato, di uso comune e leggibile meccanicamente*"** e, ove "*tecnicamente fattibile*", ottenerne la trasmissione diretta e senza impedimenti ad altro titolare indicato. Il diritto alla portabilità presuppone che il trattamento si basi sul **consenso dell'interessato** o, in alternativa, sulla base di **un contratto stipulato con l'interessato**, pertanto che il soggetto abbia "fornito" al titolare i propri dati.

Sin dall'esposta definizione, appare con chiarezza la struttura composita del diritto oggetto d'analisi:

- in primo luogo, l'interessato ha il diritto di ricevere i dati personali trattati da un titolare del trattamento e di memorizzarli su un dispositivo nella propria disponibilità in vista di un successivo utilizzo personale, senza necessità di trasferirli a un diverso titolare;
- in secondo luogo, il medesimo interessato dispone altresì del diritto di trasmettere i propri dati personali da un titolare del trattamento a un altro "senza impedimenti" o, qualora tecnicamente possibile, ottenere che i dati in oggetto siano trasferiti direttamente dal titolare originario a quello c.d. "ricevente".

Il **diritto di accesso** (art. 15) prevede che l'interessato abbia il diritto di ricevere una copia dei dati personali oggetto di trattamento.

Il **diritto all'oblio** (art. 17) si configura come il diritto alla cancellazione dei propri dati personali in forma rafforzata: il titolare, infatti, è tenuto, nel caso di esercizio di tale diritto da parte dell'interessato, ad informare della richiesta di cancellazione anche gli altri titolari che trattino i dati personali cancellati.

Il **diritto di limitazione del trattamento** (art. 18) concede all'interessato di ottenere un "blocco" del trattamento di maggiore e diversa estensione: esso è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento, ma anche nel caso in cui l'interessato chieda la rettifica dei dati o si opponga al loro trattamento.

L'esercizio dei diritti da parte dell'interessato può esser **limitato** (art. 2-*undecies* Codice Privacy) qualora dallo stesso possa derivare un pregiudizio effettivo e concreto:

a) agli interessi tutelati in base alle disposizioni in materia di riciclaggio;

b) agli interessi tutelati in base alle disposizioni in materia di sostegno alle vittime di richieste estorsive;

c) all'attività di Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;

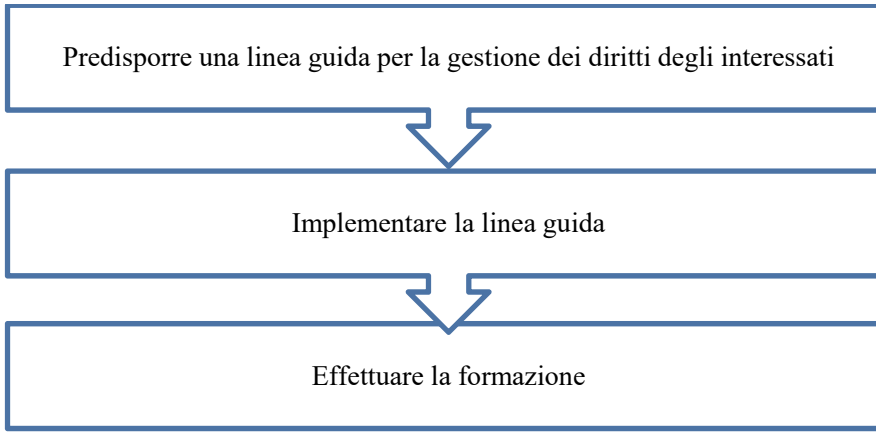
d) alle attività svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;

e) allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria;

f) alla riservatezza dell'identità del dipendente in caso di *whistleblowing* (intendendosi per esso il caso in cui un individuo – dipendente di società – denunci pubblicamente o riferisca alle autorità attività illecite o fraudolente all'interno dell'azienda – o dell'amministrazione pubblica – di appartenenza, e che possa, dunque, subire delle ripercussioni).

Infine, un breve cenno deve essere fatto con riferimento ai **diritti** riguardanti le **persone decedute**, i quali, precisa l'art. 2-*terdecies* del decreto di armonizzazione, possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione salvo, con riferimento all'offerta diretta di servizi della società dell'informazione, l'interessato lo abbia espressamente vietato con dichiarazione scritta presentata al titolare del trattamento o a quest'ultimo comunicata. Eventualmente, la volontà dell'interessato di vietare l'esercizio dei diritti deve risultare in modo non equivoco e deve essere specifica, libera e informata.

Cosa fare?


Predisporre una linea guida per la gestione dei diritti degli interessati
Implementare la linea guida
Effettuare la formazione